MaxPatrol VM

Михаил Козлов,
руководитель продукта
MaxPatrol VM

Павел Попов,
Лидер практики по
управлению уязвимостями

Управление уязвимостями с MaxPatrol VM: инструкция по применению

Что такое процесс?

Управление уязвимостями

VM

01

Следим за постоянной актуализацией данных об активах

02

Оцениваем и классифицируем активы

03

Договариваемся с IT и фиксируем политики

04

Система определяет и сортирует уязвимости

05

Следим за устранением уязвимостей и за соблюдением политик

06

Смотрим общие метрики, оцениваем тренд по компании

Asset management
Управление активами

Выделение особо опасных уязвимостей.

Оперативное реагирование на них **вне процесса**.

Процесс управления активами

Управление активами (asset management, AM) — процесс, в ходе которого выполняется формирование подробной картины IT-инфраструктуры организации, отражаемой в базе активов MaxPatrol VM, а также поддержка сведений об активах в актуальном состоянии.

Почему процесс AM важен

1. Обнаруживает активы, по которым не проводилось сканирование
2. Помогает приоритизировать сроки устранения уязвимостей (важна не только степень критичности уязвимости)
3. Повышает качество мониторинга за счет того, что предоставляет полные и актуальные сведения об активах

УПРАВЛЕНИЕ АКТИВАМИ
Инвентаризация и контроль

ВХОДНЫЕ ПАРАМЕТРЫ

- Количество и группы активов
- Уровень значимости активов
- Сведения о новых и выведенных из эксплуатации активах

Управление уязвимостями

- Выявление уязвимостей
- Анализ и приоритизация уязвимостей
- Устранение уязвимостей
- Контроль устранения уязвимостей

МОНИТОРИНГ СОБЫТИЙ ИБ

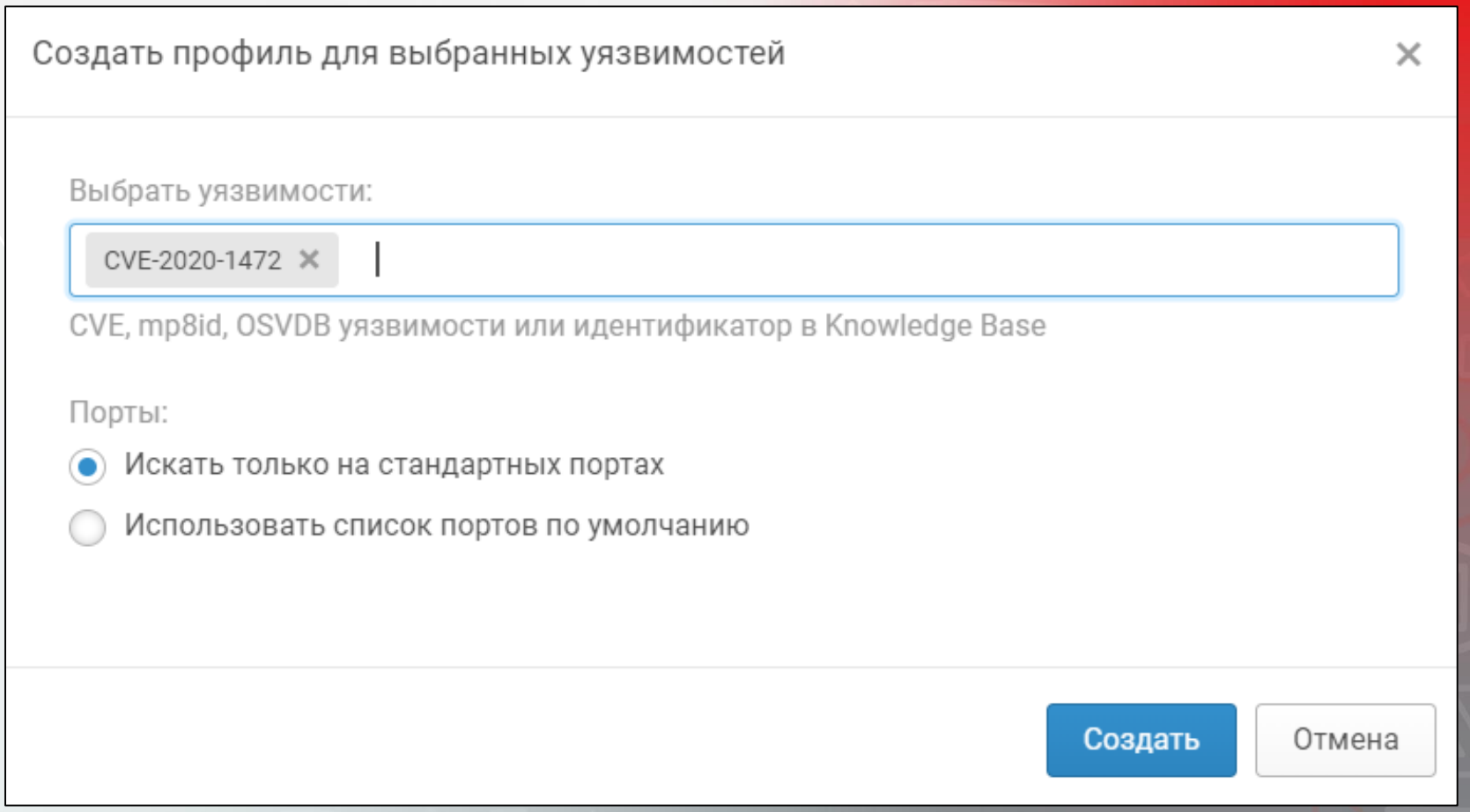
НА ДАННОМ ЭТАПЕ ВАЖНО ОПРЕДЕЛИТЬ

- Что это за актив
- Насколько сведения об активе являются полными
- Владельца / администратора актива
- Назначение актива — в каких бизнес-процессах компании он принимает участие

СПОСОБЫ СБОРА СВЕДЕНИЙ ОБ АКТИВАХ

ПРИМЕР №1

Смотрим, где в сети есть **Zerologon**, создаем точечный профиль с CVE-2020-1472

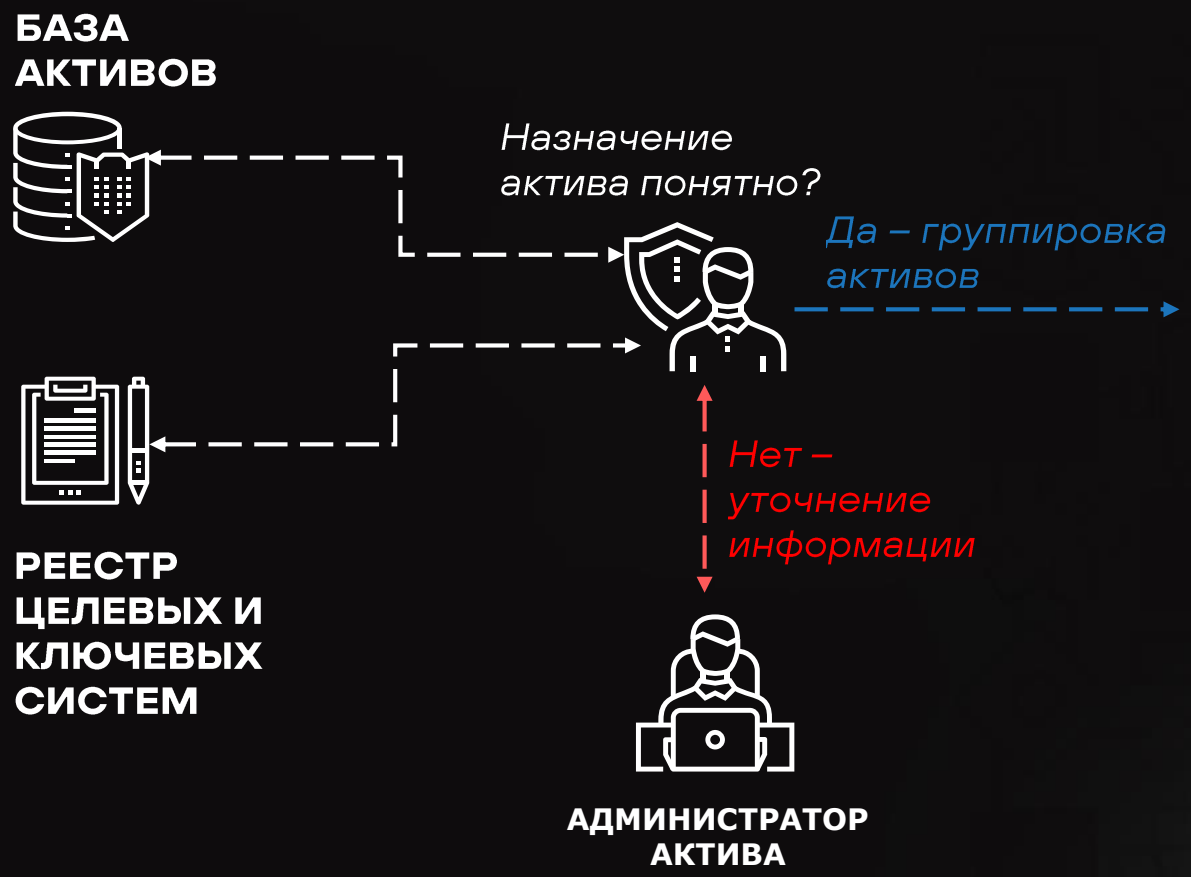


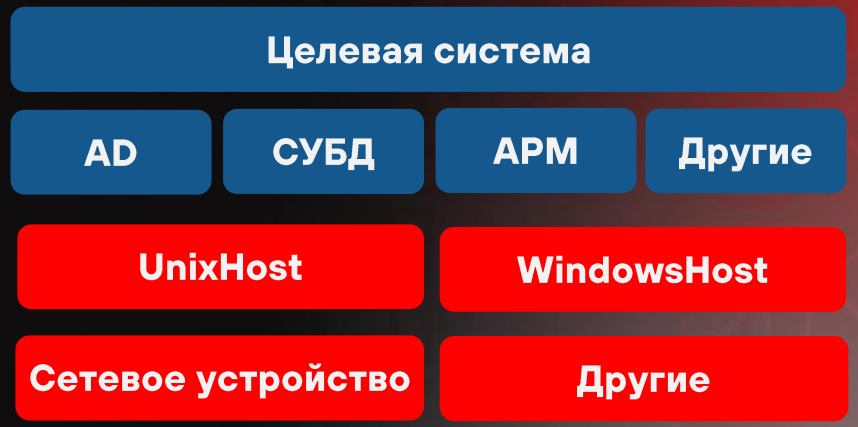
Анализ результатов сканирования

Оценка значимости активов для бизнес-процессов компании

Классификация и распределение активов по группам для автоматизации работы

Приоритизация и группировка активов





Классификация и оценка активов

MaxPatrol VM

Классификация активов

- Динамические группы
- Статические группы
- Триггеры для контроля изменений состава групп

Контроль активов

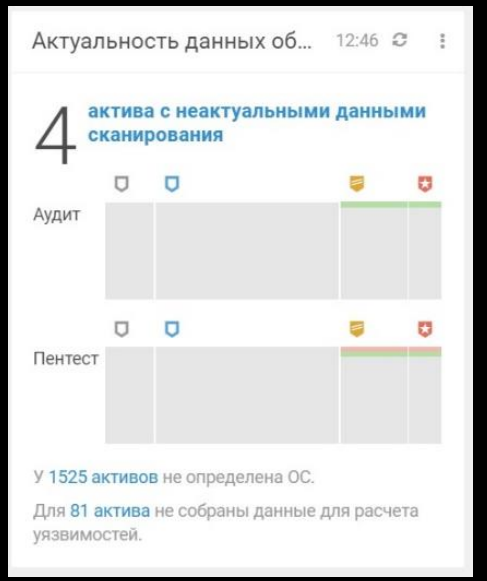
их классификации, оценка регулярности сканирования и устаревания

Распределение активов по группам

- По принадлежности к структурным подразделениям
- По принадлежности к АС
- По принадлежности к IP-сетям
- По наличию определенных ОС и ПО

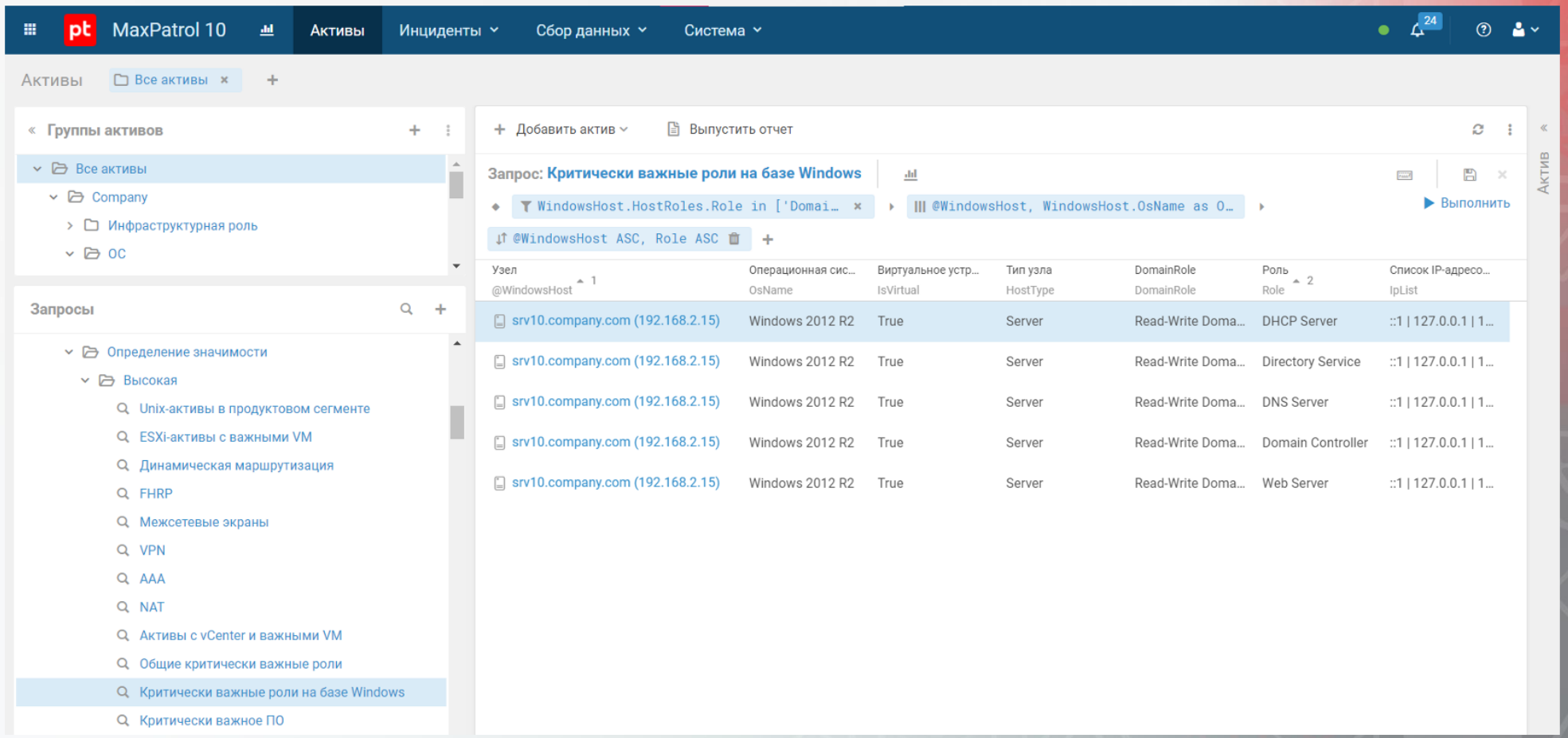
Оценка активов

задание степени важности



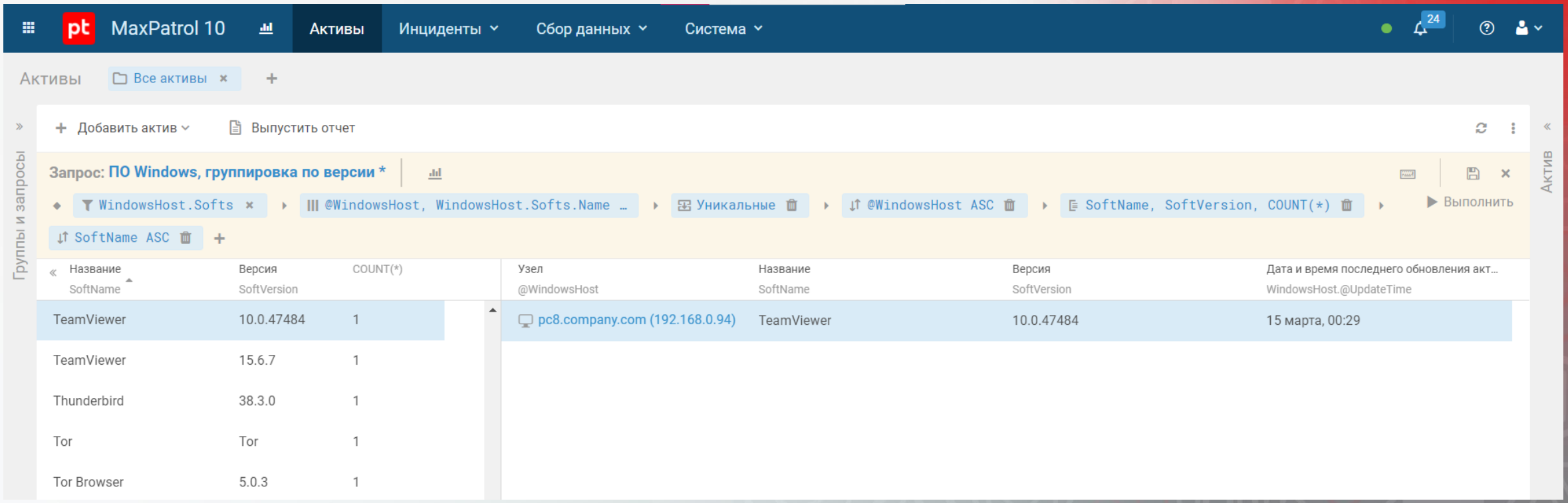
ПРИМЕР №2

Задаем всем контроллерам домена высокую значимость



ПРИМЕР №3

Находим нелегитимное или устаревшее ПО



Процесс управления уязвимостями

Управление уязвимостями (Vulnerability Management, VM) — процесс, в ходе которого выполняется сканирование инфраструктуры на предмет наличия известных уязвимостей, приоритизация уязвимостей, информирование о выявленных уязвимостях, подготовка предложений по их устранению и контроль устранения

Решаемые задачи:

ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ

Анализ информации о существующих и потенциальных уязвимостях

ОЦЕНКА ОПАСНОСТИ УЯЗВИМОСТЕЙ

Анализ и оценка влияния уязвимостей на защищенность компании

УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

Оперативное принятие мер по устранению уязвимостей

ВЫСТРАИВАНИЕ ПРОЗРАЧНЫХ ОТНОШЕНИЙ С IT-ОТДЕЛОМ

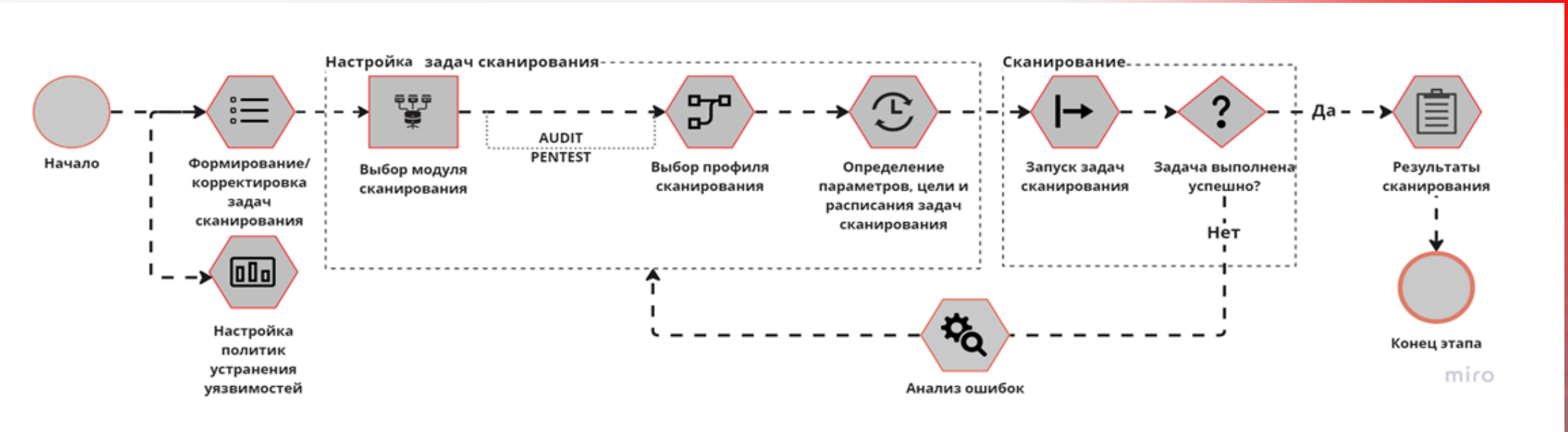
Фиксация достигнутых договоренностей

КОНТРОЛЬ УСТРАНЕНИЯ

Своевременный контроль защищенности компании

СОВЕРШЕНСТВОВАНИЕ ПРОЦЕССА

Постоянное улучшение процесса VM



Источники данных об уязвимостях

- Сведения об уязвимостях от разработчиков СЗИ, общесистемного, прикладного и специального ПО, ТС
- Общедоступные источники данных об уязвимостях (MITRE CVE, OSVDB, БДУ ФСТЭК России)

Параметры сканирования

- Периодичность сканирования
- Перечень активов для сканирования
- Профили сканирования

Рекомендации

- Процесс выявления уязвимостей должен быть постоянным, структурированным и охватывать всю IT-инфраструктуру
- Фокус на трендовые уязвимости

Классификация и приоритизация уязвимостей

MaxPatrol VM

Задание политик

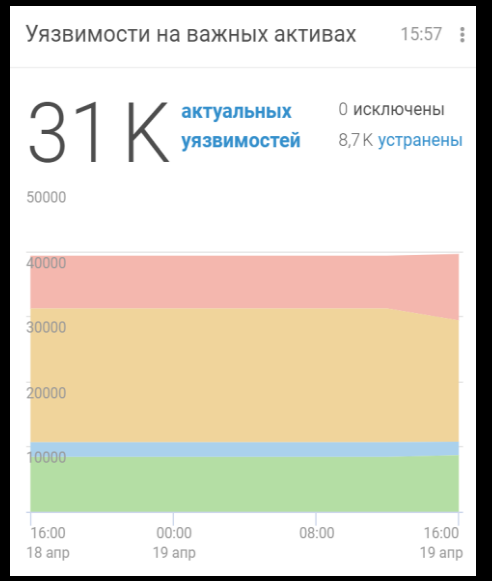
- Для планового устранения уязвимостей специалистами IT

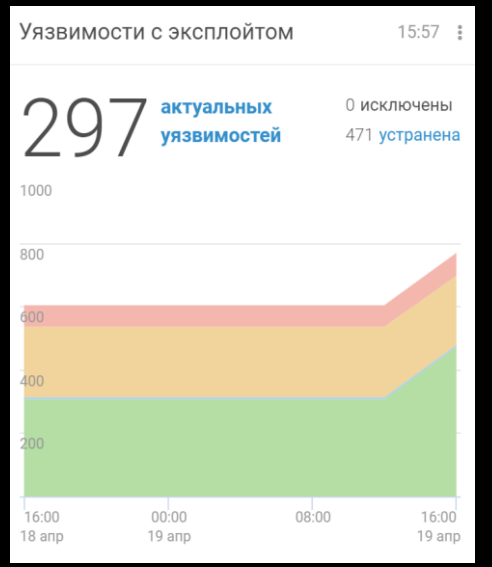
Контроль особо опасных уязвимостей

Выделяем наиболее критичные уязвимости для инфраструктуры

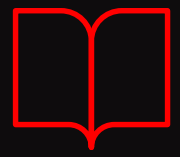
Фильтрация уязвимостей при ручном разборе

- Активы особой важности
- Уязвимости, непокрытые политиками
- Неустранимые уязвимости (с техническими ограничениями)
- 0-day



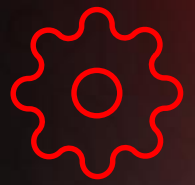


Выявляет уязвимости без сканирования



Хранит полную информацию об активах и историю изменений

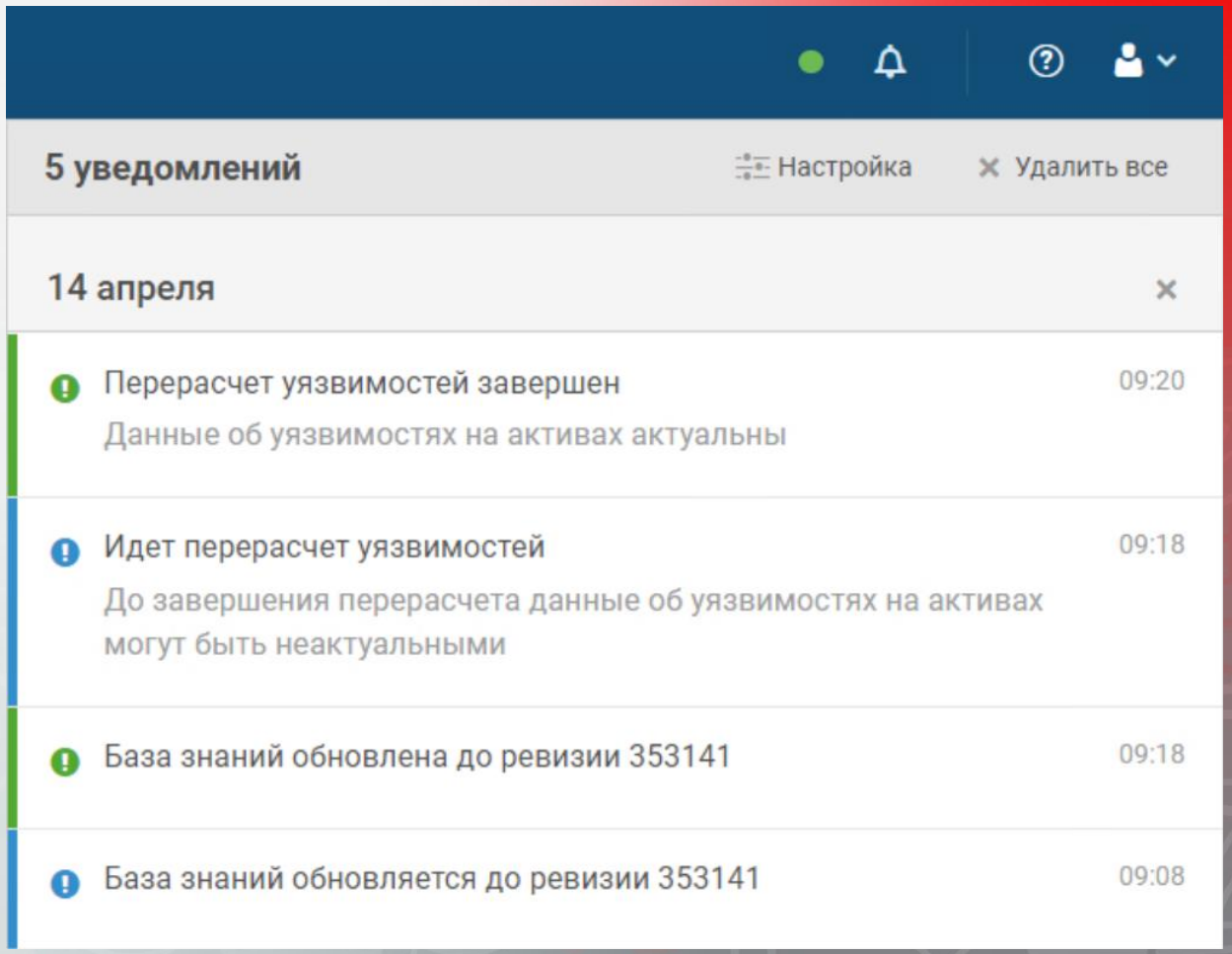
Определяет активы, используя сведения из внешних источников



Актуализирует информацию об уязвимостях автоматически после обновления базы знаний

Выявления уязвимостей без повторного сканирования

Информация об уязвимостях актуализируется автоматически после обновления базы знаний



Устранение уязвимостей

СПОСОБЫ УСТРАНЕНИЯ

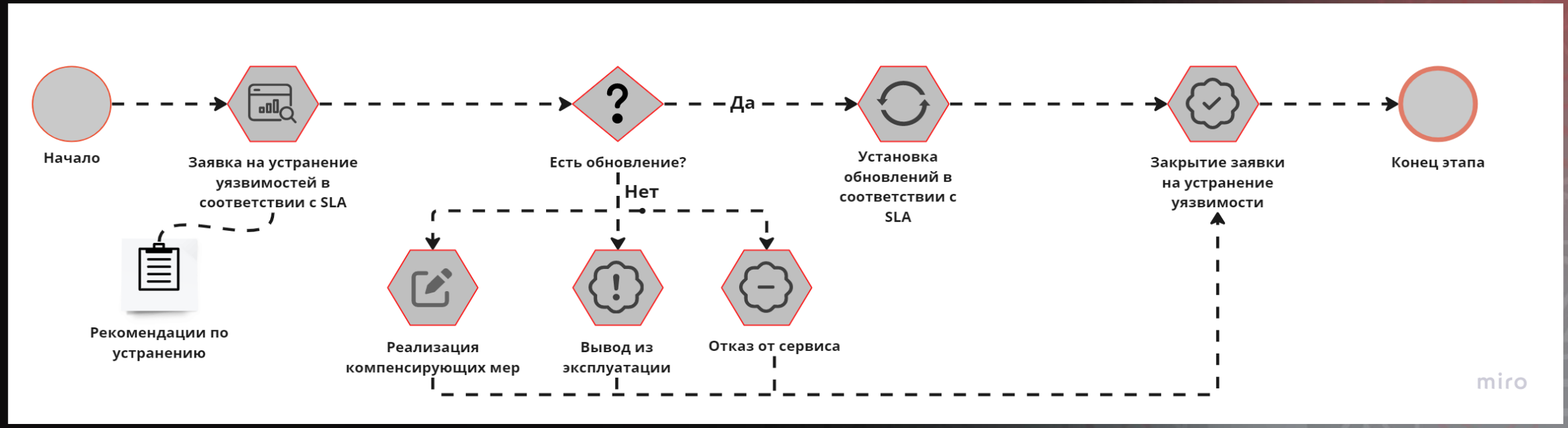
- **Обновления**
- **Компенсирующие меры**
- **Отказ от сервиса**

Плановое обновление

- ИТ устраняет уязвимости в рамках планового обновления ПО
- ИБ следит не за появлением и устранением уязвимостей, а за соблюдением договоренностей с ИТ

Внеплановое обновление

- Фокус смещается на трендовые уязвимости и те, что имеют эксплойт и расположены на важных активах
- О сроках устранения каждой уязвимости ИБ и ИТ договариваются отдельно



Трендовые уязвимости

MaxPatrol VM регулярно поставляет информацию о самых опасных уязвимостях, которые злоумышленники эксплуатируют прямо сейчас.

Опыт и знания специалистов Positive Technologies

- Пентесты
- Исследование угроз
- Расследование инцидентов ИБ

PT Knowledge Base

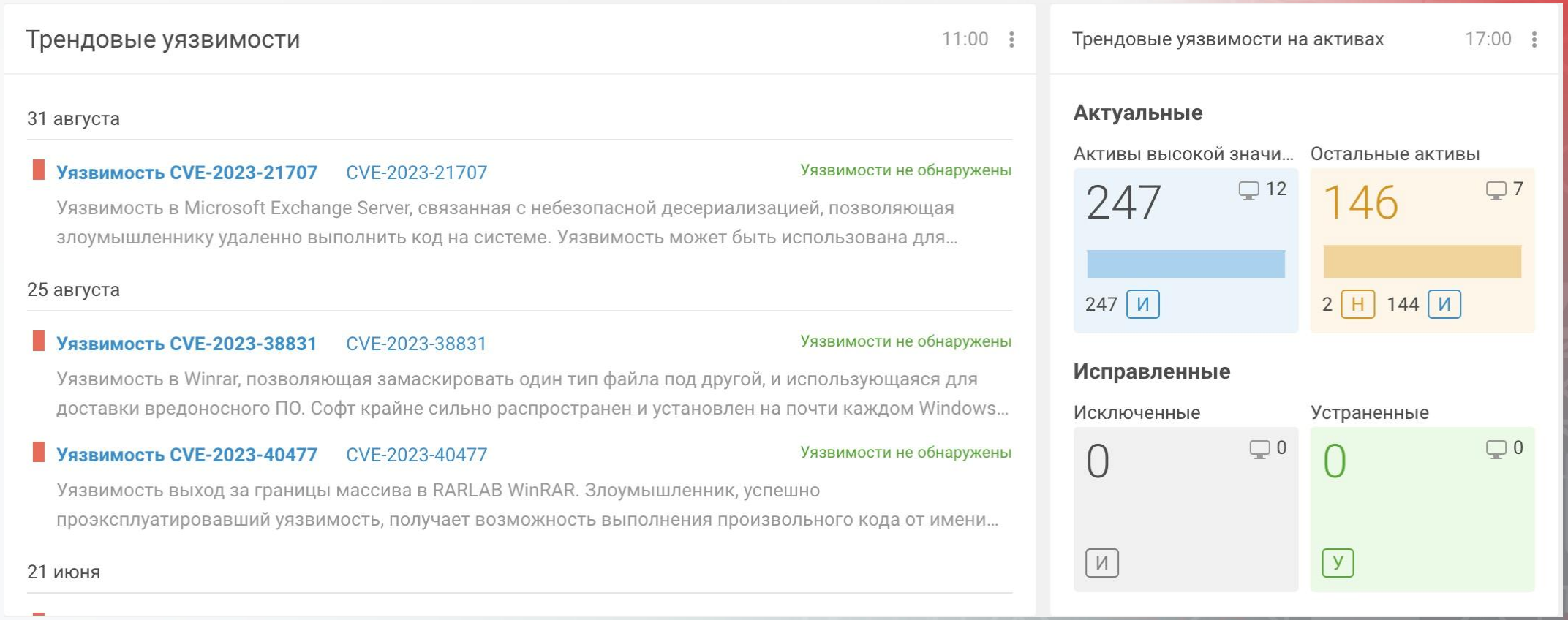
- Способы выявления и устранения уязвимостей
- Бюллетени безопасности

MaxPatrol VM

- Выявление уязвимостей
- Выделение трендовых уязвимостей
- Рекомендации по их устранению

Трендовые уязвимости

Популярны у злоумышленников и их нужно устранить в первую очередь. **В MaxPatrol VM 2.0 реализована доставка информации о трендовых уязвимостях за 12 часов!**



Контроль устранения

Контроль устранения уязвимостей вручную

Целевое состояние

Контроль устранения уязвимостей автоматизирован

Оценка соблюдения политик и устранения уязвимостей

Задание **сроков устранения уязвимостей** в зависимости от их типа и важности активов

Отслеживание динамики наличия **просроченных уязвимостей**, отдельная статистика по ООУ

Анализ устранения уязвимостей позволяет понять, нужные ли уязвимости устранялись и на тех ли активах велись работы

Комплаенс-контроль

Экспертиза Positive Technologies

Возможности

MaxPatrol VM

База знаний об уязвимостях

Построение процесса управления уязвимостями

- Обнаружение и приоритизация уязвимостей
- Контроль выявления и устранения уязвимостей

+

MaxPatrol HCC

Пакеты стандартов

Построение процесса комплаенс-контроля

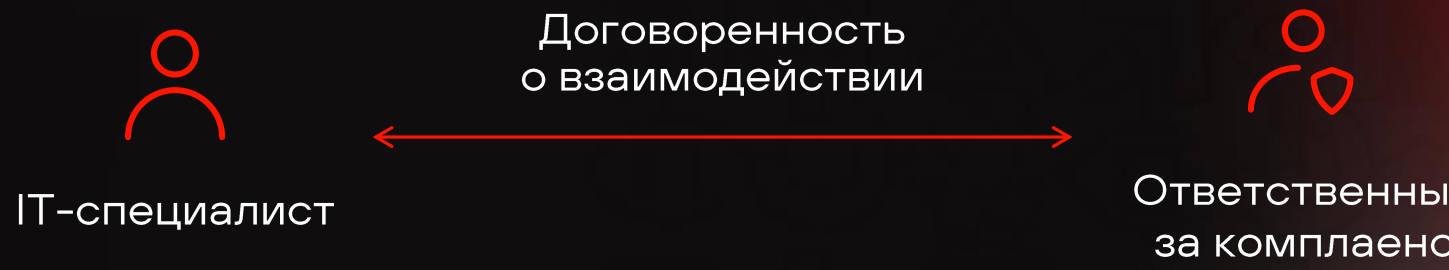
- Использование экспертных стандартов
- Возможность создавать свои критерии проверки

Основа

Security asset management

- Сбор полной информации об инфраструктуре
- Автоматическое определение активов, непрерывная актуализация данных, учет изменений

Внедрение стандартов



Регламент принятых стандартов → Выбор стандартов из регламента → Определение правил и задач по работе со стандартами → Проверка соответствия → Troubleshooting → Стандарт внедрен

Регулярный контроль соответствия стандартам

Ответственный за комплаенс

Проверка активов на соответствие стандартам

Работа с отчетом о нарушении стандартов

Подготовка новых стандартов и модификация существующих совместно со специалистом по комплаенсу

IT-специалист

Руководитель отдела ИБ

Роль MaxPatrol VM в построении процесса

Этап процесса	MaxPatrol VM
1. ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ Требуется глубокая проверка IT-инфраструктуры, выявление уязвимостей компонентов и ошибки в их конфигурации	■ Сканирует IT-инфраструктуру и собирает информацию по 3000 и более параметров ■ Выявляет версионные и конфигурационные ошибки
2. АНАЛИЗ И ПРИОРИТИЗАЦИЯ Требуется структурировать информацию о выявленных уязвимостях для более эффективного взаимодействия команд ИБ и ИТ	■ Использует правила обработки уязвимостей ■ Контролирует соблюдение политик для отслеживания SLA по устранению уязвимостей
3. УСТРАНЕНИЕ УЯЗВИМОСТЕЙ Требуется упростить и автоматизировать процесс устранения	■ Учитывает принятые компенсирующие меры ■ Позволяет настроить исключение уязвимостей ■ Передает в ИТ отчет о трендовых уязвимостях
4. КОНТРОЛЬ УСТРАНЕНИЯ Требуется обеспечить мониторинг устранения уязвимостей без лишних заявок в ИТ	■ Автоматически проверяет устранение уязвимостей по расписанию ■ Обладает настраиваемыми виджетами для отслеживания устранения уязвимостей ■ Выполняет точечные проверки для контроля устранения

Чек-лист для работы с уязвимостями

1. Согласован SLA на патч-менеджмент
2. Есть плановая и ручная обработка уязвимостей
3. Задан критерий для определения важных уязвимостей
4. Количество просроченных уязвимостей минимизировано
5. Просроченные уязвимости устраняются быстро

Курс-практикум «Как управлять уязвимостями»

Старт 22 октября

Регистрация и первый бесплатный модуль

4
недели обучения

Каждую неделю новый тематический блок с теорией, практическим заданием и тестом для проверки знаний

12
часов общения с экспертами

Каждое воскресенье с 11 до 14 часов воркшопы с экспертами, на которых участники могут задать вопросы

16
часов онлайн

Можно заниматься в удобное время

8
часов практики

Доступ к тренировочному стенду MaxPatrol VM, участники курса решают типовые задачи управления уязвимостями

Присоединяйтесь к Позитиву

Читайте нас на Хабр
habrahabr.ru/
company/pt

Узнавайте все про наши продукты
t.me/ptproductupdate

Присоединяйтесь к чату продукта
https://t.me/MPSIEMChat

Регистрируйтесь на курс по управлению уязвимостями
https://vm.edu.ptsecurity.com